Acceptable Use Policy

1. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment, internal network, internet connectivity, digital cameras and social media at The Caldecott Foundation. These rules are in place to protect employees, young people and the organisation. Inappropriate use exposes the organisation, its employees and young people to risks including ransomware, network compromise, reputational damage and data breaches.

To support understanding of acceptable use, users also need to be aware of the organisation's 'Code of Conduct' which sets out clear expectations which can be applied to the use of these technologies. All users are expected to abide by the 'Code of Conduct' whilst using these technologies which should be read in conjunction with this policy.

In addition to the overarching framework provided by the 'Code of Conduct', this policy sets out specific examples of usage which is acceptable and those which are unacceptable. This policy is not intended to set out an exhaustive list but seeks to provide guidance for users to clarify expectations.

2. Scope

This policy applies to:

- all employees, contractors, consultants, temporary staff, volunteers and others (collectively referred to as 'users') using the organisation's computer equipment (including digital cameras or smartphones), network resources or internet connectivity.
- use of any equipment that is owned or leased by the organisation and to the use of any personal devices whilst working or whilst connected to the organisation's network.
- use of digital cameras and smartphones for taking photos, videos and voice recordings.
- use personal social media, email and online accounts.

3. Acceptable Use – computer equipment, network resources and internet connectivity

The organisation's computer equipment, internal network and internet connectivity are designed to meet the legitimate needs of the organisation. Therefore, an acceptable use of the system must be aligned with a task or action which the organisation has asked a user to undertake. Users must then perform the task or action exercising due care, using training provided by the organisation and in line with the organisation's policies, procedures and protocols.

For example, a user may be writing an email to a colleague for a legitimate business reason. However, if they use offensive and discriminatory language towards their colleague in their email, they will be deemed not to be using the system in an acceptable way and be in breach of this policy.

Personal devices must never be connected by a wire to the organisation's IT network and may only be connected to the organisation's wireless (WiFi) network where it has been designated for use by guests or visitors.

3.1. Unacceptable Use – computer equipment, network resources and internet connectivity

The following activities are strictly prohibited:

- Intentionally accessing company files which the user is not authorised to access. This could be through a planned action to circumvent technical or administrative controls in place to restrict access or through an opportunistic action such as using a colleague's computer when they walk away from their desk without locking the screen.
- Using elevated privileges (those granted above the privileges held by a standard system user) to gain access to information which is not relevant to your job role or a legitimate task that you have been asked to undertake for the organisation.
- Sharing personal authentication information including an account password, PIN number, security token, Multifactor Authentication information, access card, digital certificate or other.
- Accessing the organisation's IT network or any of the organisation's cloud based systems on a device which has not been issued by the organisation.
- Setting up a forwarding rule to send some or all company emails to an email address outside of the organisation's domain.
- Downloading or viewing any pornographic or indecent material or material which could be deemed to be offensive by a reasonable person.
- Accessing a personal email account using a company issued device.
- Using a personal email account to send company information.
- Using a VPN which has not been installed by the organisation's IT team, on a company issued device which has the effect of preventing network/internet traffic from being monitored and/or filtered.
- Intentionally or negligently downloading malicious programs (viruses, worms, trojans etc.) to a device or the network which could cause disruption to or a compromise of the organisation's IT systems.
- Violating of the rights of any person or company which is protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
- Using the organisation's devices and/or IT systems to engage in the harassment, bullying, threatening, impersonation, abuse or discrimination of any individual.

- Engaging in any form of vulnerability assessment, security testing or networking penetration testing of the organisation's systems. This includes, but is not limited to, password cracking, port scanning, host scanning and packet sniffing.
- Engaging in any form of vulnerability assessment, security testing or networking penetration testing of any other individual's or organisation's systems. This includes, but is not limited to, password cracking, port scanning, host scanning and packet sniffing.
- Accessing the 'Dark Web' for any reason.
- Undertaking or engaging in any illegal activity not otherwise covered within this section.

4. Acceptable Use – digital cameras and smartphones

There are many situations where it is normal for those working with children and young people to take photos or make a video to record an event e.g. birthdays, holidays, school and sporting events. However, photos and videos of young people should only be taken on company devices and only when the appropriate consents are in place from the young person and their guardian. If in any doubt in relation to consent then please contact the organisation's data protection lead.

4.1. Unacceptable Use – digital cameras and smartphones

The following activities are strictly prohibited:

- Taking a photo or a video of a child or young person on a personal device or transferring them to a personal device.
- Taking a photo or video of a child or young person without appropriate consents in place.
- Taking a photo, video or audio recording of anyone covertly i.e. without someone's knowledge.
- Taking a photo or a video of a child or young person during incidents of challenging behaviour. The organisation does not support the practice of filming or photographing young people in distress in order to "educate" or demonstrate to them the impact of their behaviour. This practice is seen as demeaning to the young person and likely to cause further distress.

5. Acceptable Use – Personal Email, Social Media and Online Accounts

The use of social media by the organisation enables us to; attract new referrals, recruit staff, raise the organisation's profile, fundraise, seek feedback on services, celebrate the achievements of young people and staff and share knowledge and developments connected with our services.

Everyone is encouraged to engage in social media use which may promote the organisation and its values and everyone should feel part of the organisation's social media presence. However, it is also important that the use of social media does not have a negative impact on the organisation or its reputation.

The Fundraising and Communications Officer is responsible for maintaining and updating The Caldecott Foundation's digital presence, including the website and social media accounts. Part of

this responsibility includes posting material which reflects the Caldecott Foundation's views or opinions. In order to ensure that the organisation's views or opinions are not misrepresented, only the Fundraising and Communications Officer, Business Manager and CEO are authorised to submit posts on the organisation's social media platforms.

If other staff would like something to be posted or shared via the organisation's social media accounts they are encouraged to approach the Fundraising and Communications Officer at the earliest opportunity. Comments and ideas for posts, as well as feedback on previous posts, is welcomed at any time.

Individual staff may wish to share official posts made by the organisation via their own personal social media accounts. This is an appropriate and very much appreciated way of supporting the organisation to reach more people with its messages.

Anyone working for the Caldecott Foundation and using a personal social media platform must remember that they hold a professional role in the lives of the children and young people. As a result, any contributions made on these platforms should not negatively impact on that role. It is strongly advised to:

- use the platform's security and privacy settings to restrict the visibility of their information for public access online. This is a requirement for roles working directly with children and young people.
- use strong and complex passwords are used to protect accounts along with Multifactor Authentication.
- only publish content that you would be happy to share with the organisation.
- only forward or share content that you would be happy to have written yourself.
- ensure that you know who you are communicating with – false accounts can be set up pretending to be a colleague, former colleague or young person. Be vigilant and aim to confirm offline that the account is genuine.
- Avoid discussing work

5.1. Unacceptable Use – Personal Email, Social Media and Online Accounts

The following activities are strictly prohibited:

- Initiating contact with a child or young person who is currently supported by the organisation or members of their families using any personal social media, email, online account or messaging software.

  Where a child or young person initiates contact with a user's personal social media, email, online account or messaging platform the user should not respond and report the matter to the Headteacher or Responsible Individual of the relevant service. The matter can then be discussed and an appropriate plan put in place.

- Initiating contact with a child or young person who is under the age of 18 and was formerly supported by the organisation using any personal social media, email, online account or messaging software.

  Where a formerly supported child or young person over the age of 18 initiates contact with a user's personal social media, email, online account or messaging platform the user should not immediately respond but report the matter to the Headteacher or Responsible Individual of the relevant service.

  These situations can be complicated and careful thought should go into any response. Where there is agreement to engage in a conversation, this should be moved away from personal accounts and onto an organisational account wherever possible.

- Posting or sharing messages or content which provides information regarding the location of one of the organisation's registered children's homes.
- Posting or sharing messages which contain the personal or confidential information relating to a child, young person or colleague.
- Posting or sharing material which breaches the organisation's 'Code of Conduct'.

6. Exceptions

Exceptions to unacceptable use set out in sections 3, 4 and 5 may only be granted through written permission from the CEO, Business Manager, Headteacher or Responsible Individual.

7. System Monitoring and Investigation

The organisation reserves the right to log all activity which occurs on its networks, devices and software systems for legitimate business purposes. Logs may be monitored either as part of general security and maintenance tasks or in response to a specific concern. There must always be a legitimate business reason for doing so.

Any logs, monitoring or reporting may be used as part of any investigation into suspected wrongdoing or to comply with a statutory requirement. Any investigation must consider privacy concerns to ensure that the privacy rights of individuals are not breached. This includes obtaining authorisation from a senior manager to undertake searches, to limit searches to only the information which is relevant to the investigation and to redact any information of third parties.

8. Enforcement

Any employee found to have violated this policy may be subject to formal action under the organisation's Disciplinary Policy.

9. Review and Revision

This policy will be reviewed annually and may be updated as necessary to reflect changes in technology or organisational needs.